

Weekly Report 20190623

工作

- 1. 验证所提出方法的鲁棒性，并对其可解释性进行可视化
- 2. 学习联邦学习与表示学习的相关知识
- 3. 工作时长：工作日8小时，周末10小时，50h

进度

工作	内容	DDL
投稿	1.我们的方法Restricted Pooling在自然图像中(Cifar100)在不过多损失原有模型的准确率下，以端到端的方式为模型增加可解释性。并且当对图像进行扰动时，我们的方法表现了较强的鲁棒性	7.15
联邦学习与表示学习	1.阅读了关于联邦学习的论文《Secure Federated Transfer Learning》，《SecureBoost》3.阅读了一些有关偏微分方程数值解的资料	

阅读

Secure Federated Transfer Learning

通过联邦迁移学习框架，联邦内不同的成员之间可以在严守数据隐私的前提下共同挖掘数据的价值，而且可以在网络内转移补充性的数据。这样，通过利用整个数据联邦的大量有标签数据，联邦内的每个成员都可以构建出更灵活、更强大的模型；只需要对模型做微小的调整就可以看到准确率的明显提升，甚至可以比拟完全不考虑隐私、直接在全部数据上训练的表现。

SecureBoost

它可以让多个机构的学习过程共同进行，用户样本只需要有一部分相同，但可以使用完全不同的特征集，相当于对应了不同的垂直分组的虚拟数据集。SecureBoost 安全树模型的优点是，它在训练数据保持多方相互保密的前提下，可以达到和不保护隐私的方法相同的性能；而且这个过程还不需要一个共同信任的第三方参与。